Claims

What Is Claimed Is:

1. A method for initializing operation for an information security operation for an entity comprising the steps of:

obtaining data representing entity identification data;

obtaining data representing shared data associated with the entity identification data;

encrypting data, based on the shared data;

communicating in a clear text fashion, the entity identification data and the encrypted data for evaluation by an initialization authentication unit ;

comparing prestored shared data to shared data derived from the encrypted data to obtain the entity identification data; and

using the obtained entity identification data and the shared data as initialization registration data to register the entity as a proper user of the information security operation, in response to the step of comparing prestored shared data to shared data derived from the encrypted data.

2. The method of claim 1 wherein the data that is encrypted includes data representing the entity identification data.

3. The method of claim 1 wherein the data that is encrypted includes temporal data .

4. The method of claim 2 including the step of generating first data that is a function of the entity identification data, and wherein the step of encrypting data includes encrypting the first data based on the shared data.

5. The method of claim 4 including the step of generating second data that is a function of the shared data, and wherein the step of encrypting data includes encrypting the first data based on the second data.

6. The method of claim 5 wherein the first data and second data are generated using a function from the group consisting of: a one way hash function and PAKE.

7. The method of claim 1 including the step of: pre-storing the data representing the entity identification data and pre-storing the shared data, prior to the steps of obtaining.

8. The method of claim 7 including the steps of:

generating first data that is a function of the prestored data representing the entity identification data;

storing the first data with the prestored shared data as database entries;

extracting from a database entry, the prestored shared data based on the first data;

generating second data as a function of the extracted prestored shared data; and

providing the second data for use in the step of comparing.

9. The method of claim 1 wherein the shared data is shared secret data.

10. The method of claim 8 including the step of:

prior to the step of comparing, decrypting, by the initialization authentication unit, the encrypted data using the second data.

11. The method of claim 1 wherein steps of comparing prestored shared data to shared data derived from the encrypted data includes comparing data derived from the prestored shared data to data derived from the shared data.

12. A method for initializing operation for an information security operation for an entity comprising the steps of:

obtaining pre-stored data representing entity identification data ;

obtaining pre-stored data representing shared secret data associated with the entity identification data;

generating first data that is a function of the entity identification data,

generating second data that is a function of the shared secret data,

encrypting the first data based on the second data ;

communicating in a clear text fashion, the entity identification data and the encrypted first data for evaluation by an initialization authentication unit;

generating a copy of the first data as a function of the prestored data representing the entity identification data;

storing the copy of the first data with the prestored shared secret data as database entries;

extracting from a database entry, the prestored shared secret data based on communicated first data;

generating a copy of the second data as a function of the extracted prestored shared secret data ;

providing the copy of the second data for use in comparing pre-stored shared secret data to shared secret data derived from the encrypted first data to obtain the entity identification data; and

using the obtained entity identification data and the shared secret data as initialization registration data to register the entity as a proper user of the information security operation, in response to the step of comparing data derived from pre-stored shared secret data to shared secret data derived from the encrypted data.

13. The method of claim 12 wherein the pre-stored data representing entity identification data includes temporal data.

14. The method of claim 12 wherein the first data and second data are generated using a function from the group consisting of: a one way hash function, SPEKE , a block cipher encryption, a MAC, a public key encryption, or the identity function.

15. The method of claim 12 including the step of:

prior to the step of comparing, decrypting, by the initialization authentication unit, the encrypted first data using the second data based on the database entry.

16. A system for initializing operation for an information security operation for an entity comprising:

memory containing data representing entity identification data and data representing shared data associated with the entity identification data;

a first processing unit, operatively coupled to receive the data representing entity identification data and the shared data, having an encryptor that encrypts data based on the shared data and communicates in a clear text fashion, the entity identification data and the encrypted data;

an initialization authentication unit , operatively coupled to received the communicated entity identification data and the encrypted data and operatively coupled to the memory, that compares prestored shared data to shared data derived from the encrypted data to obtain the entity identification data; and uses the obtained entity identification data and the shared data as initialization registration data to register the entity as a proper user of the information security operation, in response to comparing prestored shared data to shared data derived from the encrypted data.

17. The system of claim 16 wherein the data that is encrypted includes data representing the entity identification data.

18. The system of claim 16 wherein the data that is encrypted includes temporal data .

19. The system of claim 17 wherein the first processor generates first data that is a function of the entity identification data, and encrypts the first data based on the shared data.

20. The system of claim 19 wherein the first processor generates second data that is a function of the shared data, and encrypts the first data based on the second data.

21. The system of claim 19 wherein the first data and second data are generated using a function from the group consisting of: a one way hash function, SPEKE , block cipher encryption, a MAC, public key encryption, or the identity function.

22. The system of claim 20 including a second processor operatively coupled to the memory, that generates first data that is a function of the prestored data representing the entity identification data, stores the first data with the prestored shared data as database entries, extracts from a database entry, the prestored shared data based on the first data, generates second data as a function of the extracted prestored shared data ; and provides the second data for use in comparing.

23. The system of claim 16 wherein the shared data is shared secret data.

24. The system of claim 22 wherein the initialization authentication unit includes the second processor.

25. The system of claim 22 wherein the initialization authentication unit, prior to comparing, decrypts the encrypted data using the second data.

26. The system of claim 22 wherein the initialization authentication unit, prior to comparing, encrypts shared data and compares the encrypted shared data with received encrypted data.

27. A storage medium comprising:

memory containing executable instruction that when read by one or more processing units, causes the one or more processing units to:

obtain data representing entity identification data;

obtain data representing shared data associated with the entity identification data;

encrypt data, based on the shared data;

communicate in a clear text fashion, the entity identification data and the encrypted data for evaluation by an initialization authentication unit ;

compare prestored shared data to shared data derived from the encrypted data to obtain the entity identification data; and

use the obtained entity identification data and the shared data as initialization registration data to register the entity as a proper user of the information security operation, in response to comparing prestored shared data to shared data derived from the encrypted data.

28. The storage medium of claim 27 wherein the data that is encrypted includes data representing the entity identification data.

29. The storage medium of claim 27 wherein the data that is encrypted includes temporal data .

30. The storage medium of claim 28 including memory containing executable instruction that when read by the one or more processing units, causes the one or more processing units to generate first data that is a function of the entity identification data, and encrypt the first data based on the shared data.

31. The storage medium of claim 30 including memory containing executable instruction that when read by the one or more processing units, causes the one or more processing units to generate second data that is a function of the shared data, and encrypt the first data based on the second data.

32. The storage medium of claim 31 wherein the first data and second data are generated using a function from the group consisting of: a one way hash function and PAKE.

33. The storage medium of claim 27 including memory containing executable instructions that when read by the one or more processing units, causes the one or more processing units to pre-store the data representing the entity identification data and pre-storing the shared data, prior to obtaining data representing entity identification data.

34. The storage medium of claim 33 including executable instructions that when read by the one or more processing units, causes the one or more processing units to:

generate first data that is a function of the prestored data representing the entity identification data;

store the first data with the prestored shared data as database entries;

extract from a database entry, the prestored shared data based on the first data;

generate second data as a function of the extracted prestored shared data; and

provide the second data for use in comparing prestored shared data to shared data derived from the encrypted data to obtain the entity identification data.

35. The storage medium of claim 27 wherein the shared data is shared secret data.